STATE OF VERMONT
Agency of Human Services (AHS)
Department Vermont Health Access (DVHA)

DVHA Policies for the Operation of the Vermont Health Connect	Revision History 1.0	Chapter/Number
	Effective Date: 8/28/2013	Related Documents:

Authorizing Signature: Lindsey Tucker Date Signed: 8/28/13

Lindsey Tucker, Deputy Commissioner for the Health Benefits Exchange

Vermont Health Connect (VHC) has established an information security and privacy program which satisfies the requirements for an Information Security Program as specified in the Centers for Medicare and Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E) requirements. The MARS-E baseline was established in a collaboration between CMS, the Internal Review Service (IRS); and other key stakeholders and is based on the National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53) and IRS Publication 1075. All procedures must adhere to the documents listed above and to all other applicable State and Federal Policies.

SCOPE:

This document applies to Vermont Health Connect hereafter referred as "VHC". This document also applies to contractors, including business partners, brokers, and navigators, agents, and other State-employed users of VHC.

DEFINTIONS:

Governing Entity

The governing entity refers to a body of individuals responsible for change management of VHC main application. Examples of titles include Operations Committee, Post-production Control Board or Change Control Board.

PII Definition and Data Elements

Per the Executive Office of the President, Office of Management and Budget (OMB) and the U.S. Department of Commerce, Office of the Chief Information Officer, "The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

ROLES and RESPONSIBILITIES:

Chief Information Security Officer (CISO)

- Heads an office with the mission to assist the department in achieving more secure information and information systems.
- Is ultimately responsible for the implementation of the framework in which information security resources work.

AHS Director of Information Security (AHS ISO)

The AHS ISO has the following responsibilities with respect to system and information confidentiality, integrity and availability:

- Carries out the Chief Information Security Officer security responsibilities under the ACA and serves as the primary liaison for the CISO to the AHS's Authorizing Officials, System Owners, Common Control Providers, and Enterprise Architects implementing security policies.
- Audits and evaluates security practices, reviews incidents, and reviews policy on an annual basis.
- Oversees or develops reports on remedial actions from alerts, advisories, and directives as required by the CISO and in response to requirements of OMB and US-CERT

VT CSIRT

- These responsibilities are described in the Incident Response Policy specified at http://dii.vermont.gov/sites/dii/files/pdfs/Incident-Response-Policy.pdf.

REVIEW PERIOD

This policy shall be reviewed annually and updated to reflect changes in VHC's business, administrative, or technical environments, or applicable federal/state laws and regulations. The AHS Information Security Director is responsible for overseeing the review of this policy.

POLICY:

Access Control Policy – AC-1

Access to VHC information systems shall be granted based on valid need-to-know processes. VHC must allow only authorized access to users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions

POLICY:

Security Awareness and Training Policy – AT-1

VHC will train all VHC users annually in a role-based security awareness curriculum. User access to VHC system will be contingent upon successful completion of training. The records of successful and pending completion will be available upon request.

POLICY:

Audit and Accountability Policy – AU-1

VHC shall be configured to produce, securely store and retain audit records providing for an audit trail of sufficient capacity and fidelity to allow for complete and successful investigation of suspicious events that may occur in General Support Systems (GSSs) and Major Applications (MAs) in a timely interval.

POLICY:

Security Assessment and Authorization Policy – CA-1

VHC requires that a security assessment be conducted and that a report be delivered annually to the AHS ISO. The scope of the assessment will include but not be limited to the Information Security (IS) Acceptable Risk Safeguards as described by CMS. Additionally, a security authorization must be conducted by VHC business partners as required, and a Plan of Action and Milestones report must be delivered.

POLICY:

Configuration Management Policy – CM-1

VHC and its business partners shall follow configuration management control processes as part of its application management. These processes must be documented, disseminated and updated as necessary.

POLICY:

Contingency Planning Policy – CP-1

The business partner will develop, disseminate, and periodically review/update: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination and compliance among vendoral entities, and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

POLICY:

Identification and Authentication Policy – IA-1

VHC must establish and document the minimum security requirements for the management of a user account and for password management to prevent unauthorized user access.

POLICY:

Incident Response Policy – IR-1

VHC and its business partners will execute a timely and organized response to information security incidents affecting VHC in order to enable a prompt operational recovery as well as the proper management of all legal evidence collected that is consistent with VHC System Security Plan and Special Publication 800-53 (NIST SP 800-53). VHC will coordinate its privacy and security efforts to ensure that any incident that is also a privacy breach is properly handled consistent with VHC's Incident and Breach Response Procedures, Notice of Privacy Practices, and 25 C.F.R. § 155.260.

POLICY:

System Maintenance Policy – MA-1

Maintenance activities must be documented, appropriately disseminated, and updated as necessary to facilitate implementing maintenance security controls. Such maintenance security controls include identifying and monitoring a list of maintenance tools and remote maintenance tools. A VHC governing entity must approve, control, and routinely monitor the use of information system maintenance upgrades and diagnostic activities. The GSS allows only authorized personnel to perform maintenance on the information system.

The business partners and VHC emplyees must ensure that maintenance is scheduled, performed, and documented. VHC governing entity must review records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or VHC requirements.

POLICY:

Media Protection Policy – MP-1

VHC will provide security requirements for the handling of PII/PHI/FTI processed as part of exchange operations. However, the current business process for VHC does not include the use of removable media as part of the business process

POLICY:

Physical and Environmental Protection Policy – PE-1

VHC requires both its business partners and its employees to establish the baseline requirements for the physical security management of vendor data centers so that only authorized users can access them and they are physically secured from threats and vulnerability. All vendor employees must undergo a security clearance that satisfies Federal Risk and Authorization Management Program (FEDRamp) requirements.

POLICY:

Security Planning Policy – SP-1

VHC requires both its business partners and its employees to perform due diligence and due care and take appropriate measures to safeguard information security assets for continued delivery of services that is consistent with VHC System Security Plan and the MARS-E.

POLICY:

Personnel Security Policy – PS-1

VHC requires both its business partners and its employees to establish the baseline security requirements necessary so that contractors, including business partners, brokers, and navigators; agents, and other State-employed users of VHC meet the minimum security prerequisites applicable to their function, and that they are aware of their responsibility to protect the State of Vermont's assets and information in a manner consistent with VHC System Security Plan and the MARS-E.

POLICY:

Risk Assessment Policy – RA-1

VHC requires both its business partners and its employees to identify risks, assess the impacts of the risks identified, to engage VHC in those outcomes and to take appropriate steps to reduce the identified risks to an acceptable level

POLICY:

Systems and Services Acquisition Policy – SA-1

VHC requires both its GSS business partners and its employees to establish, demonstrate and document that security is duly integrated at the first stage of any information system development or acquisition life cycle.

POLICY:

System and Communications Protection Policy – SC-1

VHC requires both its GSS business partners and its employees to establish the adequate protection of information transiting on network infrastructure and to provide for the protection of the supporting network infrastructure.

POLICY:

System and Information Integrity Policy – SI-1

VHC requires both its GSS business partners and its employees to provide adequate protection of information transiting on the vendor network infrastructure and provide adequate protection of the supporting network infrastructure in accordance with the requirements of IRS/NIST/FEDRamp guidance.

PROCEDURES:

Refer to the appropriate procedures documents for further information.